

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2003050641 A**

(43) Date of publication of application: **21.02.03**

(51) Int. Cl.
G06F 1/00
G06F 12/14
G06F 13/00
G09C 1/00
H04L 9/08
H04L 9/32
H04L 12/66

(21) Application number: **2001239396**

(22) Date of filing: **07.08.01**

(71) Applicant: **NEC CORP**

(72) Inventor: **MATSUMOTO HIDEHIRO**

(54) **PROGRAM MANAGEMENT SYSTEM, ITS
PROGRAM MANAGEMENT METHOD, AND
INFORMATION MANAGEMENT PROGRAM**

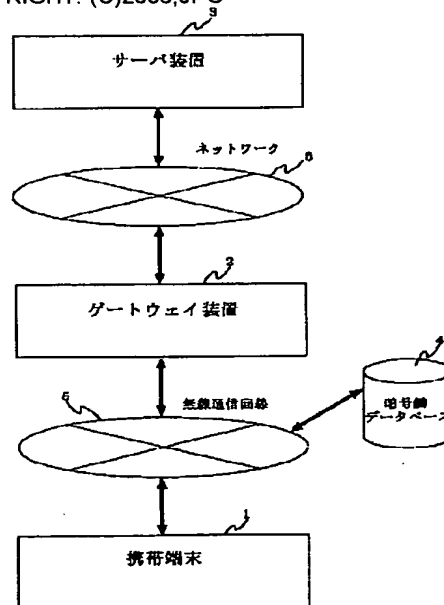
(57) Abstract:

PROBLEM TO BE SOLVED: To provide a program management system capable of preventing the intrusion of any illegal program into a portable terminal.

SOLUTION: When the certification and registration request of a program is issued from a program developer, a gateway device 2 transfers an inspection program for inspecting the validity of a program to the program developer. When informed from the program developer that the developed program has passed the inspection program the gateway device 2 accepts the registration of the developed program, registers the program, acquires a public key from a cryptographic key data base 4, adds this public key to the developed program and registers the program in a server device 3. When the acquisition request of the program is issued from a portable terminal 1, the gateway device 2 accesses the server device 3, and acquires the program to which the public key has been added, and transfers the public key to the cryptographic key data base 4 in order to perform key authentication with a private key, and downloads only

the program whose authentication has been successful to the portable terminal 1.

COPYRIGHT: (C)2003,JPO



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-50641

(P2003-50641A)

(43) 公開日 平成15年2月21日 (2003.2.21)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード* (参考)	
G 0 6 F 1/00		G 0 6 F 12/14	3 2 0 A	5 B 0 1 7
	12/14		3 5 1 Z	5 B 0 7 6
	13/00		5 3 0 A	5 B 0 8 9
		G 0 9 C 1/00	6 6 0 D	5 J 1 0 4
G 0 9 C 1/00			6 6 0 G	5 K 0 3 0

審査請求 有 請求項の数33 O L (全 14 頁) 最終頁に続く

(21) 出願番号 特願2001-239396(P2001-239396)

(22) 出願日 平成13年8月7日(2001.8.7)

(71) 出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72) 発明者 松本 英博

東京都港区芝五丁目7番1号 日本電気株式会社内

(74) 代理人 100084250

弁理士 丸山 隆夫

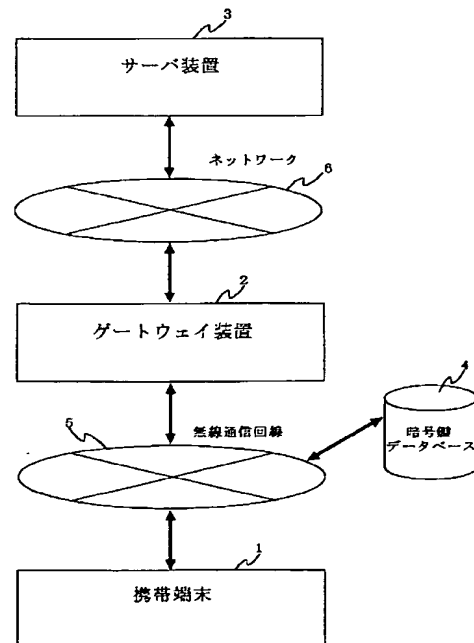
最終頁に続く

(54) 【発明の名称】 プログラム管理システム、そのプログラム管理方法、及び情報管理プログラム

(57) 【要約】

【課題】 携帯端末への不正プログラムの侵入を防止することができるプログラム管理システムを提供する。

【解決手段】 ゲートウェイ装置2は、プログラム開発者からプログラムの認定、登録申請があると、プログラムの正当性を検査する検査プログラムをプログラム開発者に転送し、当該プログラム開発者から検査プログラムに合格した旨の通知を受けると、この開発プログラムの登録を受け付け、登録し、暗号鍵データベース4から公開鍵を取得して、この公開鍵を開発プログラムに付加してサーバ装置3に登録する。また、ゲートウェイ装置2は、携帯端末1からプログラムの取得要求があると、サーバ装置3にアクセスして、公開鍵が付加されたプログラムを取得し、公開鍵を暗号鍵データベース4に転送して秘密鍵との鍵認証を実施させ、認証に合格したプログラムだけを携帯端末1にダウンロードする。



【特許請求の範囲】

【請求項1】 ネットワーク上に配置されたサーバ装置と、該サーバ装置に登録されたプログラムを前記ネットワークを介して取得し、無線通信回線を介して携帯端末に転送するゲートウェイ装置とを有するシステムであって、

前記ゲートウェイ装置は、プログラム開発者から前記サーバ装置に登録するための所定の検査プログラムに合格した旨の通知を受けると、該検査プログラムに合格した開発プログラムの登録を受け付け、前記サーバ装置に前記開発プログラムを登録することを特徴とするプログラム管理システム。

【請求項2】 前記ゲートウェイ装置は、前記開発プログラムを識別する登録番号をこの開発プログラムに付加し、前記サーバ装置に転送して登録し、前記開発プログラムに付加した登録番号を前記プログラム開発者に通知することを特徴とする請求項1記載のプログラム管理システム。

【請求項3】 ネットワーク上に配置されたサーバ装置と、該サーバ装置に登録されたプログラムを前記ネットワークを介して取得し、無線通信回線を介して携帯端末に転送するゲートウェイ装置とを有するシステムであって、

前記ゲートウェイ装置は、プログラム開発者により開発された開発プログラムに対し、登録番号を付加して前記サーバ装置に登録し、前記サーバ装置への登録後、前記プログラム開発者に前記登録番号を通知することを特徴とするプログラム管理システム。

【請求項4】 前記プログラム管理システムは、前記ゲートウェイ装置からの要求により公開鍵と秘密鍵の対を生成し、該秘密鍵を保管すると共に該公開鍵をゲートウェイ装置に転送する暗号鍵データベースを有し、前記暗号鍵データベースは、前記ゲートウェイ装置からの要求により前記公開鍵と秘密鍵の対を生成し、該公開鍵を前記ゲートウェイ装置に転送し、前記ゲートウェイ装置は、前記暗号鍵データベースより取得した前記公開鍵を前記開発プログラムに付加して前記サーバ装置に登録することを特徴とする請求項1から3の何れか一項に記載のプログラム管理システム。

【請求項5】 前記ゲートウェイ装置は、公開鍵と秘密鍵の対を生成し、前記開発プログラムに前記公開鍵を付加して前記サーバ装置に登録することを特徴とする請求項1から3の何れか一項に記載のプログラム管理システム。

【請求項6】 前記ゲートウェイ装置は、公開鍵と秘密鍵の対を生成し、前記開発プログラムを前記公開鍵で暗号化して前記サーバ装置に登録することを特徴とする請求項1から3の何れか一項に記載のプログラム管理システム。

【請求項7】 前記ゲートウェイ装置は、携帯端末からプログラムの取得要求があると、前記サーバ装置にアクセスして、前記公開鍵が付加された前記開発プログラムを取得し、取得した公開鍵を前記暗号鍵データベースに転送して前記秘密鍵との鍵認証を実施させ、認証に合格した開発プログラムだけを前記携帯端末にダウンロードすることを特徴とする請求項4記載のプログラム管理システム。

【請求項8】 前記ゲートウェイ装置は、携帯端末からプログラムの取得要求があると、前記サーバ装置にアクセスして前記公開鍵で暗号化された状態の開発プログラムを取得し、記憶した秘密鍵との鍵認証を実施して、認証に合格した開発プログラムだけを前記携帯端末にダウンロードすることを特徴とする請求項5記載のプログラム管理システム。

【請求項9】 前記ゲートウェイ装置は、携帯端末からプログラムの取得要求があると、前記サーバ装置にアクセスして前記公開鍵で暗号化された状態の開発プログラムを取得し、

記憶した秘密鍵により取得した開発プログラムを復号化して、前記携帯端末にダウンロードすることを特徴とする請求項6記載のプログラム管理システム。

【請求項10】 前記暗号鍵データベースは、前記ゲートウェイ装置から前記公開鍵を受け取ると、保持した秘密鍵で鍵認証を実施し、認証に成功すると、当該プログラムが正当なものであることを示す認定証コードを付加して前記ゲートウェイ装置に返送し、前記ゲートウェイ装置は、前記認定証コードが付加されたプログラムを携帯端末にダウンロードすることを特徴とする請求項7記載のプログラム管理システム。

【請求項11】 前記ゲートウェイ装置は、前記秘密鍵による鍵認証に成功した開発プログラムに対し、当該プログラムが正当なものであることを示す認定証コードを付加して前記携帯端末にダウンロードすることを特徴とする請求項8または9記載のプログラム管理システム。

【請求項12】 ネットワーク上に配置されたサーバ装置と、該サーバ装置に登録されたプログラムを前記ネットワークを介して取得し、無線通信回線を介して携帯端末に転送するゲートウェイ装置とを有するシステムにおけるプログラム管理方法であって、

前記ゲートウェイ装置において、プログラム開発者から前記サーバ装置に登録するための所定の検査プログラムに合格した旨の通知を受けると、該検査プログラムに合格した開発プログラムの登録を受け付け、前記サーバ装置に前記開発プログラムを登録することを特徴とするプログラム管理方法。

【請求項13】 前記ゲートウェイ装置は、前記開発プログラムを識別する登録番号をこの開発プロ

10

20

30

40

50

グラムに付加し、前記サーバ装置に転送して登録し、前記開発プログラムに付加した登録番号を前記プログラム開発者に通知することを特徴とする請求項12記載のプログラム管理方法。

【請求項14】 ネットワーク上に配置されたサーバ装置と、該サーバ装置に登録されたプログラムを前記ネットワークを介して取得し、無線通信回線を介して携帯端末に転送するゲートウェイ装置とを有するシステムにおけるプログラム管理方法であって、前記ゲートウェイ装置において、プログラム開発者により開発された開発プログラムに対し、登録番号を付加して前記サーバ装置に登録し、前記サーバ装置への登録後、前記プログラム開発者に前記登録番号を通知することを特徴とするプログラム管理方法。

【請求項15】 前記ゲートウェイ装置からの要求により公開鍵と秘密鍵の対を生成し、該秘密鍵を保管すると共に該公開鍵をゲートウェイ装置に転送する暗号鍵データベースを有し、前記暗号鍵データベースにおいて、前記ゲートウェイ装置からの要求により前記公開鍵と秘密鍵の対を生成し、該公開鍵を前記ゲートウェイ装置に転送し、前記ゲートウェイ装置において、前記暗号鍵データベースより取得した前記公開鍵を前記開発プログラムに付加して前記サーバ装置に登録することを特徴とする請求項12から14の何れか一項に記載のプログラム管理方法。

【請求項16】 前記ゲートウェイ装置において、公開鍵と秘密鍵の対を生成し、前記開発プログラムに前記公開鍵を付加して前記サーバ装置に登録することを特徴とする請求項12から14の何れか一項に記載のプログラム管理方法。

【請求項17】 前記ゲートウェイ装置において、公開鍵と秘密鍵の対を生成し、前記開発プログラムを前記公開鍵で暗号化して前記サーバ装置に登録することを特徴とする請求項12から14の何れか一項に記載のプログラム管理方法。

【請求項18】 前記ゲートウェイ装置において、携帯端末からプログラムの取得要求があると、前記サーバ装置にアクセスして、前記公開鍵が付加された前記開発プログラムを取得し、取得した公開鍵を前記暗号鍵データベースに転送して前記秘密鍵との鍵認証を実施させ、認証に合格した開発プログラムだけを前記携帯端末にダウンロードすることを特徴とする請求項15記載のプログラム管理方法。

【請求項19】 前記ゲートウェイ装置において、携帯端末からプログラムの取得要求があると、前記サーバ装置にアクセスして前記公開鍵で暗号化された状態の開発プログラムを取得し、記憶した秘密鍵との鍵認証を実施して、認証に合格した

開発プログラムだけを前記携帯端末にダウンロードすることを特徴とする請求項16記載のプログラム管理方法。

【請求項20】 前記ゲートウェイ装置において、携帯端末からプログラムの取得要求があると、前記サーバ装置にアクセスして前記公開鍵で暗号化された状態の開発プログラムを取得し、記憶した秘密鍵により取得した開発プログラムを復号化して、前記携帯端末にダウンロードすることを特徴とする請求項17記載のプログラム管理方法。

【請求項21】 前記暗号鍵データベースにおいて、前記ゲートウェイ装置から前記公開鍵を受け取ると、保持した秘密鍵で鍵認証を実施し、認証に成功すると、当該プログラムが正当なものであることを示す認定証コードを付加して前記ゲートウェイ装置に返送し、前記ゲートウェイ装置において、前記認定証コードが付加されたプログラムを携帯端末にダウンロードすることを特徴とする請求項18記載のプログラム管理方法。

【請求項22】 前記ゲートウェイ装置は、前記秘密鍵による鍵認証に成功した開発プログラムに対し、当該プログラムが正当なものであることを示す認定証コードを付加して前記携帯端末にダウンロードすることを特徴とする請求項19または20記載のプログラム管理方法。

【請求項23】 ネットワーク上に配置されたサーバ装置と、該サーバ装置に登録されたプログラムを前記ネットワークを介して取得し、無線通信回線を介して携帯端末に転送するゲートウェイ装置とを有するシステムに適用される情報管理プログラムであって、前記ゲートウェイ装置において、プログラム開発者から前記サーバ装置に登録するための所定の検査プログラムに合格した旨の通知を受けると、該検査プログラムに合格した開発プログラムの登録を受け付け、前記サーバ装置に前記開発プログラムを登録させるプログラムを実行することを特徴とする情報管理プログラム。

【請求項24】 前記ゲートウェイ装置において、前記開発プログラムを識別する登録番号をこの開発プログラムに付加し、前記サーバ装置に転送して登録させ、前記開発プログラムに付加した登録番号を前記プログラム開発者に通知させるプログラムを実行することを特徴とする請求項23記載の情報管理プログラム。

【請求項25】 ネットワーク上に配置されたサーバ装置と、該サーバ装置に登録されたプログラムを前記ネットワークを介して取得し、無線通信回線を介して携帯端末に転送するゲートウェイ装置とを有するシステムに適用される情報管理プログラムであって、前記ゲートウェイ装置において、プログラム開発者により開発された開発プログラムに対し、登録番号を付加して前記サーバ装置に登録させ、

10

20

30

40

50

前記サーバ装置への登録後、前記プログラム開発者に前記登録番号を通知させるプログラムを実行することを特徴とする情報管理プログラム。

【請求項26】 前記ゲートウェイ装置からの要求により公開鍵と秘密鍵の対を生成し、該秘密鍵を保管すると共に該公開鍵をゲートウェイ装置に転送する暗号鍵データベースを有し、

前記暗号鍵データベースにおいて、前記ゲートウェイ装置からの要求により前記公開鍵と秘密鍵の対を生成し、該公開鍵を前記ゲートウェイ装置に転送させ、前記ゲートウェイ装置において、前記暗号鍵データベースより取得した前記公開鍵を前記開発プログラムに付加して前記サーバ装置に登録させるプログラムを実行することを特徴とする請求項23から25の何れか一項に記載の情報管理プログラム。

【請求項27】 前記ゲートウェイ装置において、公開鍵と秘密鍵の対を生成し、前記開発プログラムに前記公開鍵を付加して前記サーバ装置に登録させるプログラムを実行することを特徴とする請求項23から25の何れか一項に記載の情報管理プログラム。

【請求項28】 前記ゲートウェイ装置において、公開鍵と秘密鍵の対を生成し、前記開発プログラムを前記公開鍵で暗号化して前記サーバ装置に登録させるプログラムを実行することを特徴とする請求項23から25の何れか一項に記載の情報管理プログラム。

【請求項29】 前記ゲートウェイ装置において、携帯端末からプログラムの取得要求があると、前記サーバ装置にアクセスして、前記公開鍵が付加された前記開発プログラムを取得させ、

取得した公開鍵を前記暗号鍵データベースに転送して前記秘密鍵との鍵認証を実施させ、認証に合格した開発プログラムだけを前記携帯端末にダウンロードさせるプログラムを実行することを特徴とする請求項26記載の情報管理プログラム。

【請求項30】 前記ゲートウェイ装置において、携帯端末からプログラムの取得要求があると、前記サーバ装置にアクセスして前記公開鍵で暗号化された状態の開発プログラムを取得させ、

記憶した秘密鍵との鍵認証を実施して、認証に合格した開発プログラムだけを前記携帯端末にダウンロードさせるプログラムを実行することを特徴とする請求項27記載の情報管理プログラム。

【請求項31】 前記ゲートウェイ装置において、携帯端末からプログラムの取得要求があると、前記サーバ装置にアクセスして前記公開鍵で暗号化された状態の開発プログラムを取得させ、

記憶した秘密鍵により取得した開発プログラムを復号化して、前記携帯端末にダウンロードさせるプログラムを実行することを特徴とする請求項28記載の情報管理プログラム。

【請求項32】 前記暗号鍵データベースにおいて、前記ゲートウェイ装置から前記公開鍵を受け取ると、保持した秘密鍵で鍵認証を実施し、認証に成功すると、当該プログラムが正当なものであることを示す認定証コードを付加して前記ゲートウェイ装置に返送させ、前記ゲートウェイ装置において、前記認定証コードが付加されたプログラムを携帯端末にダウンロードさせるプログラムを実行することを特徴とする請求項29記載の情報管理プログラム。

【請求項33】 前記ゲートウェイ装置において、前記秘密鍵による鍵認証に成功した開発プログラムに対し、当該プログラムが正当なものであることを示す認定証コードを付加して前記携帯端末にダウンロードさせるプログラムを実行することを特徴とする請求項30または31記載の情報管理プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ネットワーク上のサーバ装置に蓄積されたプログラムを無線通信回線を利用して通信を行なう携帯端末にダウンロードするプログラム管理システム、そのプログラム管理方法、及び情報管理プログラムに関する。

【0002】

【従来の技術】近年、携帯端末によりネットワーク（特に、インターネット）上のサーバ装置にアクセスして、情報を取得する機能を有する携帯端末が提案されている。

【0003】携帯端末への情報のダウンロードは、利用者へのサービスを豊富なものとする。例えば、音楽情報やビデオクリップの配信、秘匿性を重視する金融や商取引でのセキュリティ面での強化などが挙げられる。

【0004】図9に、この携帯端末TよりネットワークN上に存在するサーバ装置Sにアクセスするためのシステム構成の一例を示す。

【0005】図9に示されるように、携帯端末TからネットワークNにアクセスするためには、ゲートウェイ装置Gと呼ばれる専用のサーバ装置をネットワークへのアクセスポイントに設置する。

【0006】このゲートウェイ装置Gと携帯端末Tとの間は、無線通信回線で結ばれており、その無線通信回線には、例えば、無線通信回線及び携帯端末の特性に最適化されたWAP（Wireless Application Protocol）と呼ばれる通信プロトコルにより通信が行われる。また、ネットワーク上のサーバ装置Sとゲートウェイ装置Gとの間では、このネットワークNでの標準プロトコル〔インターネットであれば、インターネット標準プロトコル〔例えば、HTTP（HyperText Transfer Protocol）、TCP（Transmission Control Protocol）〕〕に基づいた通信が行われている。

【0007】ゲートウェイ装置Gは、WAPの通信プロ

トコルと、ネットワークNでの標準プロトコルのプロトコル変換機能や、データ変換機能、例えば、ネットワーク上のサーバ装置Sに保存された文書がHTML形式の文書であった場合に、このHTML形式の文書をWML(Wireless Markup Language)形式の文書に変換する機能や、ネットワークN上のサーバ装置Sに保持された文書が例えば、テキスト形式のWML文書であった場合に、バイナリ形式に変換してデータを圧縮する機能を備えている。

【0008】

【発明が解決しようとする課題】しかしながら、多種多様なサービスを提供できる反面、ダウンロードされるプログラムにエラーがあったり、悪意のあるモジュールが含まれていた場合に、携帯端末側では完全には排除できないという問題点がある。

【0009】また、場合によっては、ダウンロードしたプログラムのエラーや破壊行為を引き起こすコードが原因で、携帯電話の電話機能が利用できなくなるという問題も発生する。

【0010】このような機能不全を起こさないために、図10に示されるように携帯電話では、電話などの基本機能を実現するメモリ領域と、ダウンロードしたプログラムの格納領域とを分離して実行する環境が提案されている。

【0011】しかし、このような手段を用いても、電話機能とダウンロードプログラムの実行環境が同じ基本システム(OS)である場合、基本システムの機能にまで障害を引き起こすこともあり、完全な防衛策とはならない。

【0012】本発明は上記事情に鑑みてなされたものであり、携帯端末への不正プログラムの侵入を防止することができるプログラム管理システム、そのプログラム管理方法、及び情報管理プログラムを提供することを目的とする。

【0013】

【課題を解決するための手段】係る目的を達成するために請求項1記載の発明は、ネットワーク上に配置されたサーバ装置と、該サーバ装置に登録されたプログラムをネットワークを介して取得し、無線通信回線を介して携帯端末に転送するゲートウェイ装置とを有するシステムであって、ゲートウェイ装置は、プログラム開発者からサーバ装置に登録するための所定の検査プログラムに合格した旨の通知を受けると、該検査プログラムに合格した開発プログラムの登録を受け付け、サーバ装置に開発プログラムを登録することを特徴とする。

【0014】請求項2記載の発明は、請求項1記載の発明において、ゲートウェイ装置は、開発プログラムを識別する登録番号をこの開発プログラムに付加し、サーバ装置に転送して登録し、開発プログラムに付加した登録番号をプログラム開発者に通知することを特徴とする。

【0015】請求項3記載の発明は、ネットワーク上に配置されたサーバ装置と、該サーバ装置に登録されたプログラムをネットワークを介して取得し、無線通信回線を介して携帯端末に転送するゲートウェイ装置とを有するシステムであって、ゲートウェイ装置は、プログラム開発者により開発された開発プログラムに対し、登録番号を付加してサーバ装置に登録し、サーバ装置への登録後、プログラム開発者に登録番号を通知することを特徴とする。

10 【0016】請求項4記載の発明は、請求項1から3の何れか一項に記載の発明において、プログラム管理システムは、ゲートウェイ装置からの要求により公開鍵と秘密鍵の対を生成し、該秘密鍵を保管すると共に該公開鍵をゲートウェイ装置に転送する暗号鍵データベースを有し、暗号鍵データベースは、ゲートウェイ装置からの要求により公開鍵と秘密鍵の対を生成し、該公開鍵をゲートウェイ装置に転送し、ゲートウェイ装置は、暗号鍵データベースより取得した公開鍵を開発プログラムに付加してサーバ装置に登録することを特徴とする。

20 【0017】請求項5記載の発明は、請求項1から3の何れか一項に記載の発明において、ゲートウェイ装置は、公開鍵と秘密鍵の対を生成し、開発プログラムに公開鍵を付加してサーバ装置に登録することを特徴とする。

【0018】請求項6記載の発明は、請求項1から3の何れか一項に記載の発明において、ゲートウェイ装置は、公開鍵と秘密鍵の対を生成し、開発プログラムを公開鍵で暗号化してサーバ装置に登録することを特徴とする。

30 【0019】請求項7記載の発明は、請求項4記載の発明において、ゲートウェイ装置は、携帯端末からプログラムの取得要求があると、サーバ装置にアクセスして、公開鍵が付加された開発プログラムを取得し、取得した公開鍵を暗号鍵データベースに転送して秘密鍵との鍵認証を実施させ、認証に合格した開発プログラムだけを携帯端末にダウンロードすることを特徴とする。

40 【0020】請求項8記載の発明は、請求項5記載の発明において、ゲートウェイ装置は、携帯端末からプログラムの取得要求があると、サーバ装置にアクセスして公開鍵で暗号化された状態の開発プログラムを取得し、記憶した秘密鍵との鍵認証を実施して、認証に合格した開発プログラムだけを携帯端末にダウンロードすることを特徴とする。

【0021】請求項9記載の発明は、請求項6記載の発明において、ゲートウェイ装置は、携帯端末からプログラムの取得要求があると、サーバ装置にアクセスして公開鍵で暗号化された状態の開発プログラムを取得し、記憶した秘密鍵により取得した開発プログラムを復号化して、携帯端末にダウンロードすることを特徴とする。

50 【0022】請求項10記載の発明は、請求項7記載の

発明において、暗号鍵データベースは、ゲートウェイ装置から公開鍵を受け取ると、保持した秘密鍵で鍵認証を実施し、認証に成功すると、当該プログラムが正当なものであることを示す認定証コードを付加してゲートウェイ装置に返送し、ゲートウェイ装置は、認定証コードが付加されたプログラムを携帯端末にダウンロードすることを特徴とする。

【0023】請求項11記載の発明は、請求項8または9記載の発明において、ゲートウェイ装置は、秘密鍵による鍵認証に成功した開発プログラムに対し、当該プログラムが正当なものであることを示す認定証コードを付加して携帯端末にダウンロードすることを特徴とする。

【0024】請求項12記載の発明は、ネットワーク上に配置されたサーバ装置と、該サーバ装置に登録されたプログラムをネットワークを介して取得し、無線通信回線を介して携帯端末に転送するゲートウェイ装置とを有するシステムにおけるプログラム管理方法であって、ゲートウェイ装置において、プログラム開発者からサーバ装置に登録するための所定の検査プログラムに合格した旨の通知を受けると、該検査プログラムに合格した開発プログラムの登録を受け付け、サーバ装置に開発プログラムを登録することを特徴とする。

【0025】請求項13記載の発明は、請求項12記載の発明において、ゲートウェイ装置は、開発プログラムを識別する登録番号をこの開発プログラムに付加し、サーバ装置に転送して登録し、開発プログラムに付加した登録番号をプログラム開発者に通知することを特徴とする。

【0026】請求項14記載の発明は、ネットワーク上に配置されたサーバ装置と、該サーバ装置に登録されたプログラムをネットワークを介して取得し、無線通信回線を介して携帯端末に転送するゲートウェイ装置とを有するシステムにおけるプログラム管理方法であって、ゲートウェイ装置において、プログラム開発者により開発された開発プログラムに対し、登録番号を付加してサーバ装置に登録し、サーバ装置への登録後、プログラム開発者に登録番号を通知することを特徴とする。

【0027】請求項15記載の発明は、請求項12から14の何れか一項に記載の発明において、ゲートウェイ装置からの要求により公開鍵と秘密鍵の対を生成し、該秘密鍵を保管すると共に該公開鍵をゲートウェイ装置に転送する暗号鍵データベースを有し、暗号鍵データベースにおいて、ゲートウェイ装置からの要求により公開鍵と秘密鍵の対を生成し、該公開鍵をゲートウェイ装置に転送し、ゲートウェイ装置において、暗号鍵データベースより取得した公開鍵を開発プログラムに付加してサーバ装置に登録することを特徴とする。

【0028】請求項16記載の発明は、請求項12から14の何れか一項に記載の発明において、ゲートウェイ装置において、公開鍵と秘密鍵の対を生成し、開発プロ

グラムに公開鍵を付加してサーバ装置に登録することを特徴とする。

【0029】請求項17記載の発明は、請求項12から14の何れか一項に記載の発明において、ゲートウェイ装置において、公開鍵と秘密鍵の対を生成し、開発プログラムを公開鍵で暗号化してサーバ装置に登録することを特徴とする。

【0030】請求項18記載の発明は、請求項15記載の発明において、ゲートウェイ装置において、携帯端末からプログラムの取得要求があると、サーバ装置にアクセスして、公開鍵が付加された開発プログラムを取得し、取得した公開鍵を暗号鍵データベースに転送して秘密鍵との鍵認証を実施させ、認証に合格した開発プログラムだけを携帯端末にダウンロードすることを特徴とする。

【0031】請求項19記載の発明は、請求項16記載の発明において、ゲートウェイ装置において、携帯端末からプログラムの取得要求があると、サーバ装置にアクセスして公開鍵で暗号化された状態の開発プログラムを取得し、記憶した秘密鍵との鍵認証を実施して、認証に合格した開発プログラムだけを携帯端末にダウンロードすることを特徴とする。

【0032】請求項20記載の発明は、請求項17記載の発明において、ゲートウェイ装置において、携帯端末からプログラムの取得要求があると、サーバ装置にアクセスして公開鍵で暗号化された状態の開発プログラムを取得し、記憶した秘密鍵により取得した開発プログラムを復号化して、携帯端末にダウンロードすることを特徴とする。

【0033】請求項21記載の発明は、請求項18記載の発明において、暗号鍵データベースにおいて、ゲートウェイ装置から公開鍵を受け取ると、保持した秘密鍵で鍵認証を実施し、認証に成功すると、当該プログラムが正当なものであることを示す認定証コードを付加してゲートウェイ装置に返送し、ゲートウェイ装置は、認定証コードが付加されたプログラムを携帯端末にダウンロードすることを特徴とする。

【0034】請求項22記載の発明は、請求項19または20記載の発明において、ゲートウェイ装置において、秘密鍵による鍵認証に成功した開発プログラムに対し、当該プログラムが正当なものであることを示す認定証コードを付加して携帯端末にダウンロードすることを特徴とする。

【0035】請求項23記載の発明は、ネットワーク上に配置されたサーバ装置と、該サーバ装置に登録されたプログラムをネットワークを介して取得し、無線通信回線を介して携帯端末に転送するゲートウェイ装置とを有するシステムに適用される情報管理プログラムであって、ゲートウェイ装置において、プログラム開発者からサーバ装置に登録するための所定の検査プログラムに合

10

20

30

40

50

格した旨の通知を受けると、該検査プログラムに合格した開発プログラムの登録を受け付け、サーバ装置に開発プログラムを登録させるプログラムを実行することを特徴とする。

【0036】請求項24記載の発明は、請求項23記載の発明において、ゲートウェイ装置において、開発プログラムを識別する登録番号をこの開発プログラムに付加し、サーバ装置に転送して登録させ、開発プログラムに付加した登録番号をプログラム開発者に通知させるプログラムを実行することを特徴とする。

【0037】請求項25記載の発明は、ネットワーク上に配置されたサーバ装置と、該サーバ装置に登録されたプログラムをネットワークを介して取得し、無線通信回線を介して携帯端末に転送するゲートウェイ装置とを有するシステムに適用される情報管理プログラムであって、ゲートウェイ装置において、プログラム開発者により開発された開発プログラムに対し、登録番号を付加してサーバ装置に登録させ、サーバ装置への登録後、プログラム開発者に登録番号を通知させるプログラムを実行することを特徴とする。

【0038】請求項26記載の発明は、請求項23から25の何れか一項に記載の発明において、ゲートウェイ装置からの要求により公開鍵と秘密鍵の対を生成し、該秘密鍵を保管すると共に該公開鍵をゲートウェイ装置に転送する暗号鍵データベースを有し、暗号鍵データベースにおいて、ゲートウェイ装置からの要求により公開鍵と秘密鍵の対を生成し、該公開鍵をゲートウェイ装置に転送させ、ゲートウェイ装置において、暗号鍵データベースより取得した公開鍵を開発プログラムに付加してサーバ装置に登録させるプログラムを実行することを特徴とする。

【0039】請求項27記載の発明は、請求項23から25の何れか一項に記載の発明において、ゲートウェイ装置において、公開鍵と秘密鍵の対を生成し、開発プログラムに公開鍵を付加してサーバ装置に登録させるプログラムを実行することを特徴とする。

【0040】請求項28記載の発明は、請求項23から25の何れか一項に記載の発明において、ゲートウェイ装置において、公開鍵と秘密鍵の対を生成し、開発プログラムを公開鍵で暗号化してサーバ装置に登録させるプログラムを実行することを特徴とする。

【0041】請求項29記載の発明は、請求項26記載の発明において、ゲートウェイ装置において、携帯端末からプログラムの取得要求があると、サーバ装置にアクセスして、公開鍵が付加された開発プログラムを取得させ、取得した公開鍵を暗号鍵データベースに転送して秘密鍵との鍵認証を実施させ、認証に合格した開発プログラムだけを携帯端末にダウンロードさせるプログラムを実行することを特徴とする。

【0042】請求項30記載の発明は、請求項27記載

の発明において、ゲートウェイ装置において、携帯端末からプログラムの取得要求があると、サーバ装置にアクセスして公開鍵で暗号化された状態の開発プログラムを取得させ、記憶した秘密鍵との鍵認証を実施して、認証に合格した開発プログラムだけを携帯端末にダウンロードさせるプログラムを実行することを特徴とする。

【0043】請求項31記載の発明は、請求項28記載の発明において、ゲートウェイ装置において、携帯端末からプログラムの取得要求があると、サーバ装置にアクセスして公開鍵で暗号化された状態の開発プログラムを取得させ、記憶した秘密鍵により取得した開発プログラムを復号化して、携帯端末にダウンロードさせるプログラムを実行することを特徴とする。

【0044】請求項32記載の発明は、請求項29記載の発明において、暗号鍵データベースにおいて、ゲートウェイ装置から公開鍵を受け取ると、保持した秘密鍵で鍵認証を実施し、認証に成功すると、当該プログラムが正当なものであることを示す認定証コードを付加してゲートウェイ装置に返送させ、ゲートウェイ装置において、認定証コードが付加されたプログラムを携帯端末にダウンロードさせるプログラムを実行することを特徴とする。

【0045】請求項33記載の発明は、請求項30または31記載の発明において、ゲートウェイ装置において、秘密鍵による鍵認証に成功した開発プログラムに対し、当該プログラムが正当なものであることを示す認定証コードを付加して携帯端末にダウンロードさせるプログラムを実行することを特徴とする。

【0046】

【発明の実施の形態】次に、添付図面を参照しながら本発明のプログラム管理システム、そのプログラム管理方法、及び情報管理プログラムに係る実施の形態を詳細に説明する。図1～図8を参照すると本発明のプログラム管理システム、そのプログラム管理方法、及び情報管理プログラムに係る実施形態が示されている。

【0047】図1に示されるように本発明に係る実施形態は、クライアント装置としての携帯端末1と、ネットワークでの通信プロトコルと無線通信回線での通信プロトコルとのプロトコル変換を行うゲートウェイ装置2と、ネットワーク上に設けられたサーバ装置3と、無線通信回線に接続された暗号化鍵データベース4とを有して構成される。携帯端末1とゲートウェイ装置2とは無線通信回線にて接続され、ゲートウェイ装置2とサーバ装置3とはインターネット等のネットワークに接続されている。また、ゲートウェイ装置2と暗号鍵データベース4とは無線通信回線で接続されている。

【0048】クライアント装置としての携帯端末1は、特定のプログラムを内蔵し、そのプログラムを実行できるものであって、ゲートウェイ装置2と無線通信回線を介して接続する。また、携帯端末1は、ゲートウェイ装

10

20

30

40

50

置2を介してインターネット等のネットワーク6上のサーバ装置3に接続する。また、携帯端末1は、サーバ装置3に蓄積されたプログラムを取得し、正常に動作する（利用可能となる）状態となった場合に、表示画面にこの旨を通知する機能を有する。

【0049】ゲートウェイ装置2は、内部にサーバ装置3から取得したプログラム、またはプログラム開発者から転送されたプログラムを一時的に蓄積する記憶部（キャッシュメモリ等で構成する）を有する。また、サーバ装置3に登録したプログラムを特定する登録番号を発行する登録番号発生機能と、公開鍵と登録番号の付いたプログラムをネットワークを介して適当なサーバ装置3に転送する通信機能を備えている。なお、ゲートウェイ装置2は、これらの機能以外にプロトコル変換機能や、データ変換機能、例えば、サーバ装置に保持された文書がHTML形式の文書であった場合に、このHTML形式の文書をWAPで用いられるWML形式の文書に変換する機能を持ち合わせる。

【0050】サーバ装置3は、ゲートウェイ装置2から転送される、公開鍵の付いたプログラム及びデータと、これらに該当する登録番号とを登録する。

【0051】暗号化鍵データベース4は、ゲートウェイ装置2からの依頼により公開鍵と秘密鍵の対を発生し、その内部に秘密鍵を保管する。また、ゲートウェイ装置2からの依頼により鍵認証を行ない、認証が正常に終了すると、認証されたプログラムが正当なものであることを示す認定証を発行する機能を有する。なお、暗号化データベース4は、通信事業者などによって管理、運営され、その登録内容は非公開である（特に、本システムの利用者、ゲートウェイ装置管理者、サーバ装置事業者に対しては非公開である）。

【0052】上記構成からなる本実施形態は、インターネット等のネットワークへのアクセス機能を有する携帯端末1が、ネットワーク上のサーバ装置3からプログラムやデータをダウンロードする際に、このプログラムに不備やシステムの破壊行為を狙ったモジュールが含まれていることで、携帯端末1の基本機能（電話機能等）が不全になるといった不具合を防止することを目的としている。

【0053】この目的を達成するための本実施形態による動作手順を図2、3に示されたフローチャート、及び図4～8を参照しながら説明する。本実施形態は、プログラム開発者が開発したプログラムに対し、所定の検査プログラムを用いてこのプログラムが正当なものであるかを評価する。プログラム開発者よりプログラムの認定、及び登録申請があると（ステップS1）、以下の検査仕様を満たす検査プログラムをプログラム開発者に配布する。そして、プログラム開発者に自身の開発したプログラムの検査を行なわせる（ステップS2）。なお、本実施形態では、プログラム開発者からの開発プログラ

ムの認定、登録申請は、ゲートウェイ装置2に対して行なわれるが、サーバ管理者、ゲートウェイ管理者、無線通信事業者、あるいはダウンロードサービスに顧客への製造物責任を持つ事業者（以下、事業者という）に対して行なうものであってもよい。

【0054】検査プログラムの検査仕様は、少なくともプログラムとデータのコードに関する検査（コード検査）と、適用する携帯端末の属性（画面の大きさ、色数、入力方法、回線速度、通信実行速度など）に適したコード規則に適合しているか否かを調べる検査（テンプレート検査）とからなる。また、コード検査は、少なくとも、コードの文法的な誤りがないかを調べる文法検査、ダウンロード機能以外の基本システム（OS）に直接関与するネイティブ関数の呼び出しがないかを検査するライブラリ検査と、プログラムの実行作業領域が携帯端末の内蔵メモリの与えられた範囲を超えず、異常処理が多重に発生してもメモリの利用領域を超えないなどのメモリ利用規則からなる。

【0055】上述した検査項目からなる検査に合格すると（ステップS3／YES）、プログラム開発者は、検査に合格したプログラムをゲートウェイ装置2に登録する（ステップS4）。ゲートウェイ装置2は、プログラム開発者よりアップロードされたプログラムを一時的に記憶部に蓄積し、暗号化データベース4に暗号化鍵の取得要求を出す（ステップS5）。図4には、プログラム開発者により開発されたプログラムをゲートウェイ装置2に登録する状態が示されている。

【0056】暗号化データベース4は、ゲートウェイ装置2からの依頼により公開鍵と秘密鍵の対を生成し、秘密鍵を内部に保管すると共に公開鍵を無線通信回線を介してゲートウェイ装置2に転送する。図5には、暗号化データベース4により生成された公開鍵がゲートウェイ装置2に転送された状態が示されている。

【0057】暗号化データベース4から公開鍵を取得したゲートウェイ装置2は、プログラムを識別するための登録番号を生成し、この登録番号と公開鍵とをプログラムに付加してネットワーク6上のサーバ装置3にアップロードする（ステップS6）。サーバ装置3はゲートウェイ装置2から公開鍵と登録番号が付加されたプログラムを自身の記憶部に登録する（ステップ7）と共に、このプログラムを正常に登録したことをゲートウェイ装置2に通知する。図6には、暗号化されたプログラムがサーバ装置3に転送され、登録された状態が示されている。

【0058】ゲートウェイ装置2は、サーバ装置3からの登録通知を受け取ると、認定、及び登録申請をしていたプログラム開発者に登録の完了とプログラムに付けられた登録番号を通知する（ステップS8）。登録番号をプログラム開発者に通知した時点でゲートウェイ装置2は、当該登録プログラムのダウンロードサービスを開始

する(ステップS9)。ここまでの処理でプログラムの登録までの一連の処理を終了する。

【0059】次に、クライアント装置としての携帯端末1からのアクセスにより、サーバ装置3に登録されたプログラムを当該携帯端末1にダウンロードする手順を説明する。

【0060】無線通信回線5を介して携帯端末1からのプログラムの取得要求を受けたゲートウェイ装置2(ステップS11/YES)は、サーバ装置3にアクセスして、該当するプログラムの取得要求を行なう(ステップS12)。サーバ装置3は、ゲートウェイ装置2からのプログラム取得要求により、公開鍵と登録番号が付加されている該当プログラムをゲートウェイ装置2に転送する。図7には、ゲートウェイ装置2がサーバ装置3から該当プログラムの転送を受け、記憶部に蓄積した状態が示されている。

【0061】サーバ装置2から該当するプログラムを取得したゲートウェイ装置2は(ステップS13/YES)、携帯端末1にプログラムのダウンロードの一時停止を通知し、暗号鍵データベース4に、プログラムに付加された公開鍵の認証を依頼する(ステップS14)。暗号鍵データベース4は、ゲートウェイ装置2から公開鍵を取得し、記憶した秘密鍵で鍵認証を行い、転送されたプログラムが正当なものであるか否かを検証する。

【0062】鍵認証によりプログラムが正当なものであると判断すると、暗号鍵データベース4は、そのプログラムが正当なものであることを示す認定証コードをゲートウェイ装置2に送信する。また、鍵認証に失敗した場合には、このプログラムが正当なものではない旨をゲートウェイ装置2に通知する。

【0063】ゲートウェイ装置2は、暗号鍵データベース4より認定証を受けると(ステップS15)、この認定証を付加したプログラムを携帯端末1にダウンロードする(ステップS16)。また、暗号鍵データベース4より該当プログラムが不正なものであるとの認定を受けると、携帯端末1に対し、取得要求のあったプログラムは不正なものであり、このプログラムのダウンロードはできない旨を通知する(ステップS17)。図8には、暗号鍵データベース4により正当なプログラムであると認定されたプログラムが携帯端末1にダウンロードされた状態が示されている。

【0064】このように本実施形態は、検査プログラムによる検査に合格したプログラムだけをサーバ装置3に登録することにより、システムの破壊を狙った悪意のあるプログラムを排除し、携帯端末1の機能不全を招くようなプログラム、データをダウンロードする不具合を防止することができる。

【0065】また、本構成では、プログラムは、常にゲートウェイ装置2の監視を通じてのみサーバ装置3に登録するため、不特定のプログラム開発者がサーバ装置3

に異常のあるプログラムを登録することができない。従って、サーバ装置3の保全を図ることもできる。

【0066】また、万一、異常のあるプログラムを検査に合格したと偽ってプログラム開発者が申請しても、登録番号を付加することで、異常のあったプログラムをサーバ装置3から即座に削除することができ、また、プログラム開発者を特定して被害を最小限に食い止めることができる。

【0067】また、利用者に認定証コード付きのプログラムをダウンロードすることで、利用者に正当なプログラムであることを認識させ安心感を提供する共に、海賊版の排除など著作権の保護に利用することができる。

【0068】また、検査プログラムを予め公開することで、プログラム開発者が、合格への習熟度を上げることができる。また、登録番号をプログラム開発者に通知することで、プログラム開発者自ら検査した検査プログラムを本システムの事業者が追認したことになる。従って、検査プログラムの精度の向上を見込むことができる。

【0069】また、本システムの事業者は、従来の登録プログラムの全数検査を避けることができるばかりでなく、ゲートウェイ装置でダウンロードプログラムを一括管理することができ経済的な負担を軽減することができる。

【0070】また、秘密鍵の管理を暗号鍵データベース4を管理する無線通信事業者が行なうことで、ゲートウェイ装置の公開鍵の管理も間接的に行なわれることから、ゲートウェイ装置2とサーバ装置3、その間の通信網の管理が不要となる。

【0071】なお、上述した実施形態は、本発明の好適な実施の形態である。但し、これに限定されるものではなく、本発明の要旨を逸脱しない範囲内で種々変形実施が可能である。例えば、上述した実施形態では、ゲートウェイ装置2が1つのサーバ装置3と接続している場合を例に説明したが、複数のサーバ装置と接続するネットワークを利用した接続形態であっても同様の効果を得ることができる。また、上記実施形態では、公開鍵方式を用いて認証を行なっているが、無線ネットワークシステム固有のセキュリティシステムを利用しても同様な効果を得ることができる。

【0072】また、ゲートウェイ装置と暗号鍵データベース4とは無線通信回線にて接続されているが、有線の専用回線で接続してもよいし、インターネット等のネットワークを介して接続するものであってもよい。また、ゲートウェイ装置2に暗号鍵データベース4の機能を持たせ、ゲートウェイ装置2で公開鍵の発生、認定証コードを発行するものであってもよい。

【0073】また、ゲートウェイ装置2に暗号鍵データベース4の機能を持たせる他の例として、ゲートウェイ装置2は、プログラム開発者よりプログラムがアップロ

ードされると、自身で公開鍵と秘密鍵の対を発生し、公開鍵でこのプログラムを暗号化してサーバ装置3に登録する。携帯端末1よりアクセスがあった場合には、サーバ装置3から暗号化された状態のプログラムの転送を受け、自身で記憶している秘密鍵でこのプログラムを復号化する。そして、復号化に成功した場合には、認定証を発行して携帯端末1にダウンロードするものであってもよい。

【0074】また、本発明の情報管理プログラムに係る実施形態は、図1に示されたゲートウェイ装置2、サーバ装置3、暗号鍵データベース4に、図2、3に示された手順、または、段落番号73で説明した手順で制御するプログラムを格納することで実現できる。

【0075】

【発明の効果】以上の説明より明らかなように本発明は、検査プログラムによる検査に合格したプログラムだけをサーバ装置に登録することにより、システムの破壊を狙った悪意のあるプログラムを排除し、携帯端末の機能不全を招くようなプログラム、データをダウンロードする不具合を防止することができる。

【0076】また、本構成では、プログラムは、常にゲートウェイ装置の監視を通じてのみサーバ装置に登録するため、不特定のプログラム開発者が、サーバ装置に異常のあるプログラムに登録することができない。従って、サーバ装置の保全を図ることもできる。

【0077】また、万一、異常のあるプログラムを検査に合格したと偽ってプログラム開発者が申請しても、登録番号を付加することで、該当プログラムをサーバ装置から即座に削除することができ、また、プログラム開発者を特定して被害を最小限に食い止めることができる。

【0078】また、利用者に認定証コード付きのプログラムをダウンロードすることで、利用者に正当なプログラムであることを認識させ安心感を提供する共に、海賊版の排除など著作権の保護に利用することができる。

【0079】また、検査プログラムを予め公開すること

で、プログラム開発者が、合格への習熟度を上げることができる。また、登録番号をプログラム開発者に通知することで、プログラム開発者自ら検査した検査プログラムを本システムの事業者が追認したことになる。従って、検査プログラムの精度の向上を見込むことができる。

【0080】また、本システムの事業者は、従来の登録プログラムの全数検査を避けることができるばかりでなく、ゲートウェイ装置でダウンロードプログラムを一括管理することができ経済的な負担を軽減することができる。

【0081】また、秘密鍵の管理を暗号鍵データベースを管理する無線通信事業者が行なうことで、ゲートウェイ装置の公開鍵の管理も間接的に行なわれることから、ゲートウェイ装置とサーバ装置、その間の通信網の管理が不要となる。

【図面の簡単な説明】

【図1】本発明に係る実施形態の構成を表すブロック図である。

【図2】動作手順を示すフローチャートである。

【図3】動作手順を示すフローチャートである。

【図4】動作手順を説明するための図である。

【図5】動作手順を説明するための図である。

【図6】動作手順を説明するための図である。

【図7】動作手順を説明するための図である。

【図8】動作手順を説明するための図である。

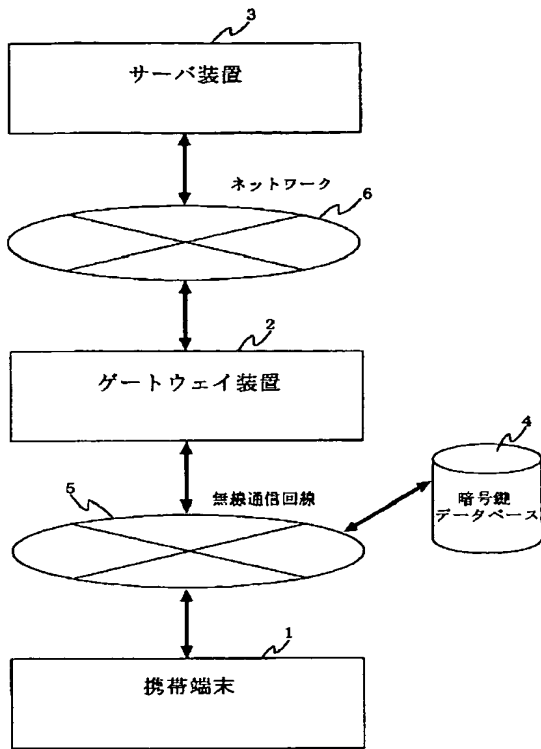
【図9】従来のシステム構成図である。

【図10】従来の問題点を説明するための図である。

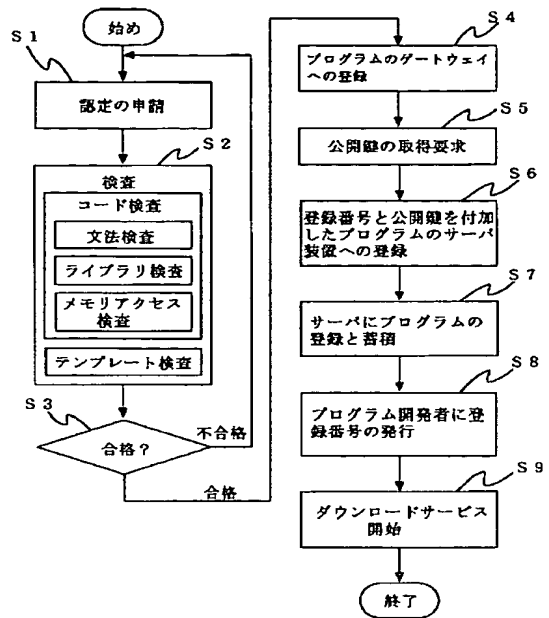
【符号の説明】

- 1 携帯端末
- 2 ゲートウェイ装置
- 3 サーバ装置
- 4 暗号鍵データベース
- 5 無線通信回線
- 6 ネットワーク

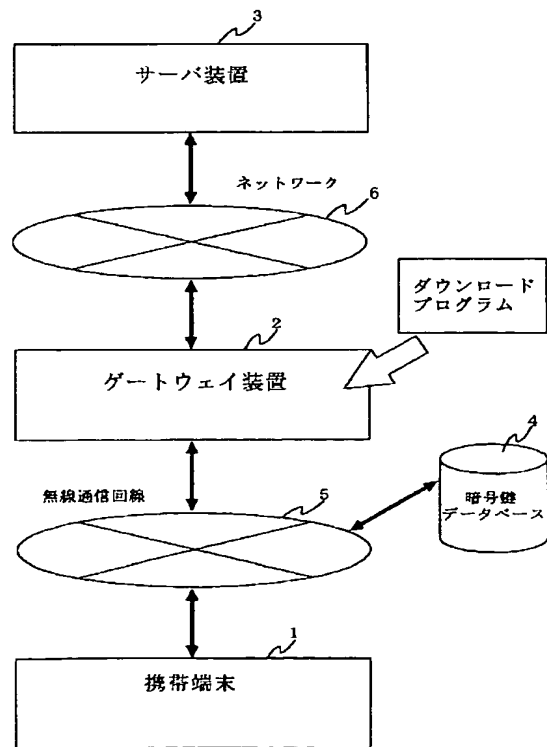
【図1】



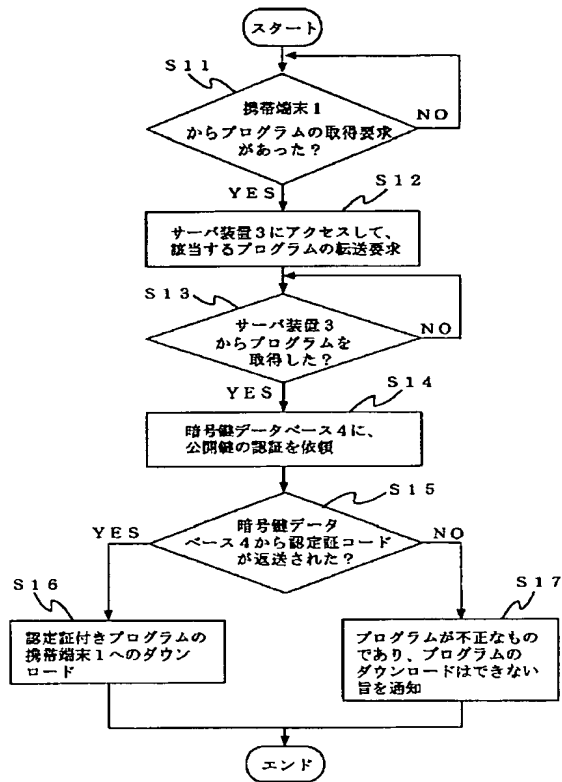
【図2】



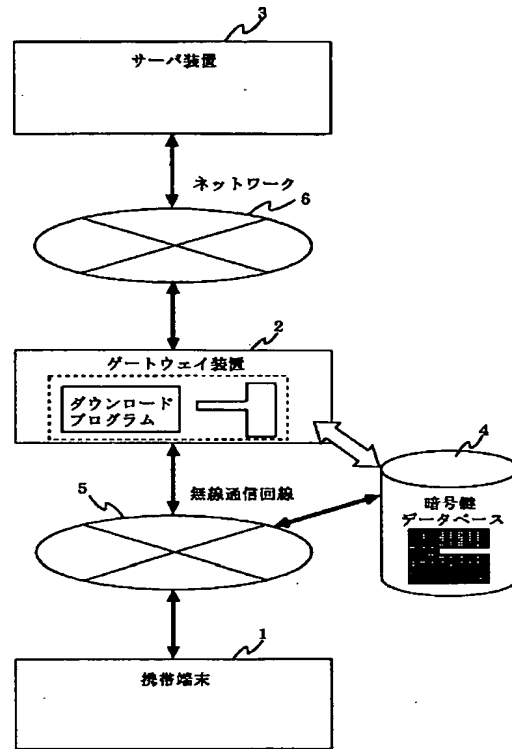
【図4】



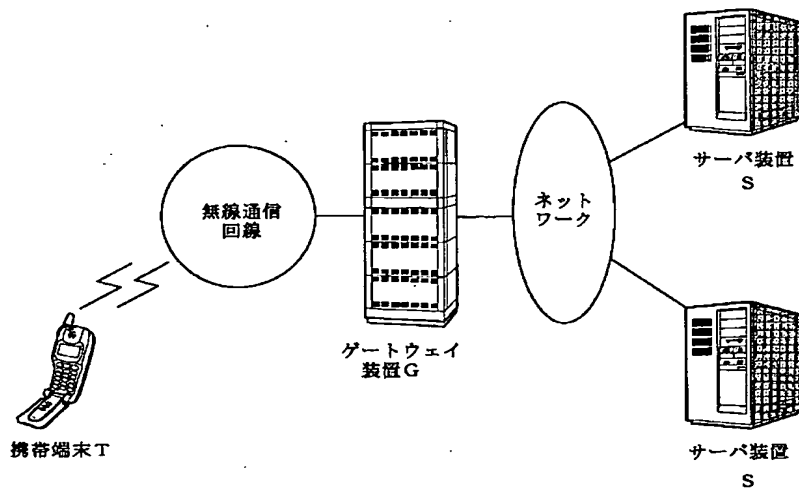
【図3】



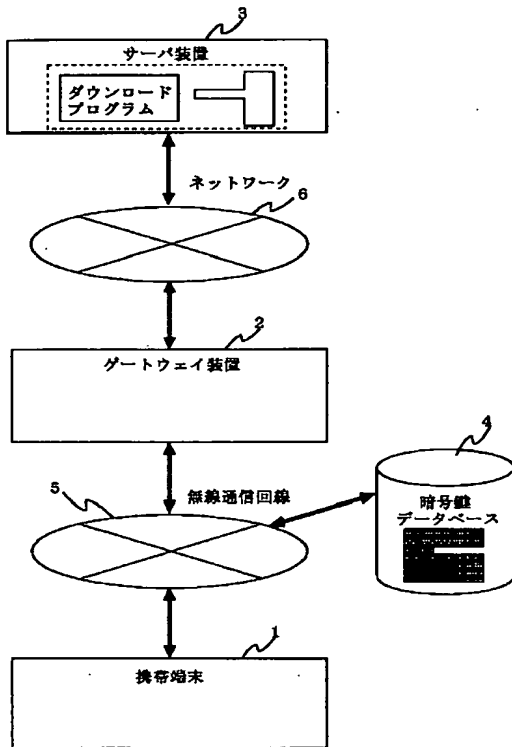
【図5】



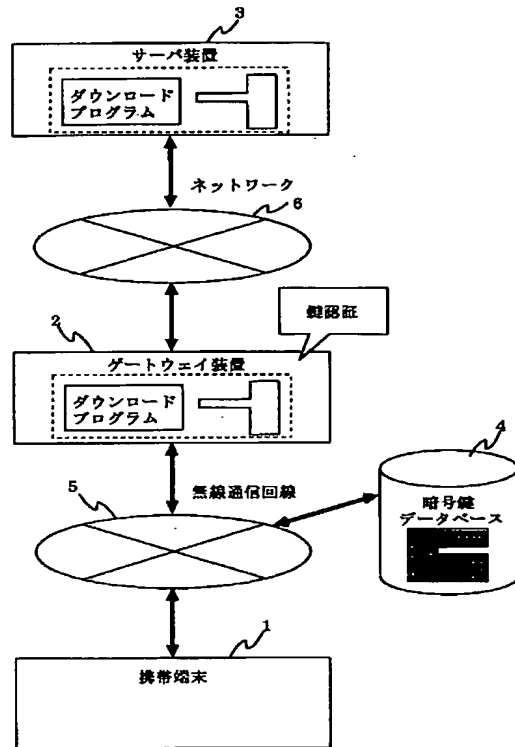
【図9】



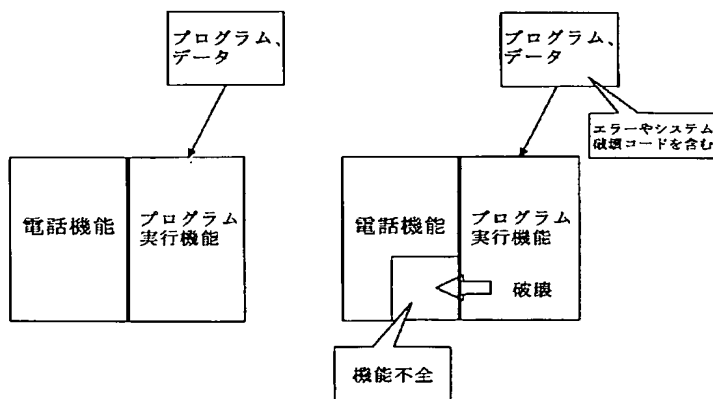
【図6】



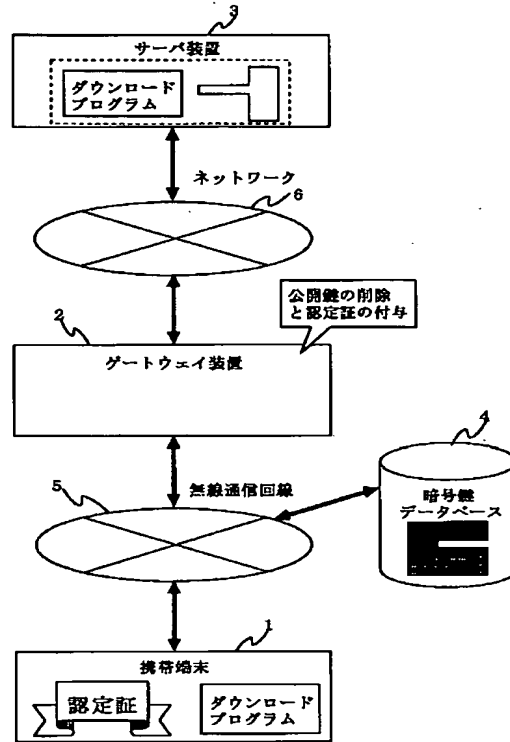
【図7】



【図10】



【図8】



フロントページの続き

(51)Int.Cl.⁷

G 0 9 C 1/00
H 0 4 L 9/08
9/32
12/66

識別記号

F I

H 0 4 L 12/66
G 0 6 F 9/06
H 0 4 L 9/00

テーマコード (参考)

B
6 6 0 G
6 7 5 B
6 0 1 F

F ターム (参考) 5B017 AA08 BA07 CA15
5B076 FA13 FB02 FB03
5B089 GA11 JB07 KH30
5J104 JA21 NA02 PA07
5K030 GA15 HA08 HB19 HC01 HC09
HD03 HD05 JL01 JL07 JT01
JT03 KA01 KA07 KA13 LD19